Information Services Board Briefing Paper on the Updated Statewide Information Technology Security Policy and Practices

Prepared by Mary Lou Griffith, DIS/MOSTD, (360) 902-2978.

Description

Digital government requires a secure and trustworthy environment for conducting sensitive transactions through open networks. To that end, the Information Services Board (ISB) initiated a comprehensive review and update of the statewide information technology (IT) Security Policy to address the security issues of conducting electronic commerce across the state enterprise. An IT and Internet Security Program Charter was developed and approved at the June 12, 2001, ISB meeting. A recommendation that an Independent Security Analyst be assigned to report the status of the state's IT Security Program on a recurring basis was also approved by the Board at that time. Mr. Jeff Scheel was named as the ISB Independent Security Analyst and will report to the Board the current status of the IT Security program.

Background

Washington State government has been recognized as a leader in applying digital technologies and the Internet in service to the citizen. This has been achieved by leveraging the open architecture of the Internet to provide access to a wide range of public information and services.

Using the Internet to its greatest advantage requires a higher degree of security than was the case in an earlier era of closed systems and proprietary networks. Washington State government must take sufficient steps to ensure that citizens and businesses interacting with public agencies are protected by the appropriate information technology security. Beyond a range of anonymous exchanges available through the Internet, citizens and businesses need secure access to look up their medical or other benefit claims, exchange sensitive health records, or make or receive electronic payments with government. All these transactions require secure access control and data protection for the electronic exchange of information over the Internet. This is being done through the state's secure gateway, Transact Washington, which implements trustworthy access control through Public-Key Infrastructure (PKI).

Washington State government has set clear direction and minimum standards for the way in which sensitive information and transactions are protected by state agencies. The policies, standards, and guidelines set the preconditions for achieving a consistent and reliable set of protections for sensitive information within a shared, trusted environment.

Status

In accordance with the ISB IT Security Policy, all executive and judicial branch agencies and educational institutions under the purview of the ISB were required to submit Information Security Policy Compliance letters by October 6, 2001. A template letter was made available online at the IT Portfolio Management web site. It was used by the agencies to describe the status of their program and define the tasks that must be completed for full compliance prior to the due date of the annual security validation letter due June 30, 2002. The letters were to indicate each agency's status regarding steps taken to comply with the ISB IT Security Policy.

A total of 44 letters have been received. An analysis of the letters indicates the following compliance status:

- Agencies indicating they are currently compliant: 3
- Agencies indicating they have developed or are developing a plan for compliance: 34
- Agencies with incomplete plans: 7

Two positive trends were noted in the content of the letters:

- Several agencies indicated they had appointed or intended to appoint an IT Security Manager.
- Many agencies provided detailed security program development plans.

As tools and training vehicles are made available to state agencies, focus will be given to mitigating these issues.

Issues

- The Governor is advocating legislative changes to bolster state response to emergency incidents.

- Some agencies addressed the potential impact of budgetary constraints on the development of comprehensive IT security programs.

- Additional guidance may be needed on the development and implementation of effective Security Awareness Training.

- Many agencies identified significant work to be completed by June 30, 2002. The availability of adequate resources to complete the tasks was not addressed so the associated level of risk is difficult to discern.

- The state has established the Washington Computer Incident Reporting Center (WACIRC) to provide a coordinated response to IT security incidents and thefts.

- A new Technical Architecture Advisory Group (TAAG) Subcommittee is being established to develop standards for network connected computers to help address the prevention, detection, recovery and mitigation of computer incidents caused by computer viruses and worms.

Recommendation

DIS recommends that the Independent Security Analyst continue to report regularly to the Board on the status of the state's IT Security program and that the Board receive status of the agencies' security programs in the monthly update reports.